



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/521,858	01/21/2005	Franciscus Lucas Antonius Kamperman	NL 020681	1225
24737 7590 01/22/2009 PHILIPS INTELLECTUAL PROPERTY & STANDARDS P.O. BOX 3001 BRIARCLIFF MANOR, NY 10510				
			EXAMINER SCHWARTZ, DARREN B	
			ART UNIT 2435	PAPER NUMBER
			MAIL DATE 01/22/2009	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary**Application No.**

10/521,858

Applicant(s)KAMPERMAN, FRANCISCUS
LUCAS ANTONIUS**Examiner**

DARREN SCHWARTZ

Art Unit

2435

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 December 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3,5-11 and 13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3,5-11 and 13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Claims 1, 3, 5-11 and 13 are presented for examination. The claims are not amended.

Response to Arguments

Applicant's arguments filed 31 December 2008 have been fully considered but they are not persuasive.

1. In response to applicant's argument that "...the HOST CONTROLLER should be identified with the first communication device as claimed, while the STORAGE SUBSYSTEM PORT ADAPTER should be identified with the second communication device as claimed" (page 7 of REMARKS), the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985).

2. In response to applicant's argument that "...the HOST CONTROLLER should be identified with the first communication device as claimed, while the STORAGE SUBSYSTEM PORT ADAPTER should be identified with the second communication device as claimed" (page 7 of REMARKS), the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the

references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

3. Applicant argues that the combination of Lundkvist and Blumenau et al are silent to teaching: *generating by the first communication device a third signal by modifying the first signal according to the common secret; comparing the third signal with the received second signal to check if the second signal has been modified according to the common secret.*

The Examiner disagrees. Blumenau teaches: generating by the first communication device [Figure 33, element "STORAGE SUBSYSTEM PORT ADAPTER"] a third signal [Figure 33, element "ENCRYPT THE RANDOM NUMBER USING THE PORT ADAPTER'S COPY OF THE HOST CONTROLLER'S KEY"] by modifying the first signal according to the common secret [Figure 33, elements 383 & 385: "SEND RANDOM NUMBER AND REQUEST FOR VERIFICATION TO THE HOST CONTROLLER" & "ENCRYPT THE RANDOM NUMBER USING THE PORT ADAPTER'S COPY OF THE HOST CONTROLLER'S KEY"] (col 37, lines 55-59: "*In step 384, the host controller receives the random number and the request for verification from the port adapter. In step 385, the port adapter encrypts the random number with its copy of the host controller's key;*" col 37, lines 62-66: "*For example, the encryption could use the well-known method of the Data Encryption Standard (DES), or any sequence of encryption operations, for example, substitution, blocking, permutation, expansion, and compaction.*"); comparing the third signal [Figure 33, element: 385;

"ENCRYPT THE RANDOM NUMBER USING THE PORT ADAPTER'S COPY OF THE HOST CONTROLLER'S KEY"] with the received second signal [Figure 33, element: 387 & 388; "SEND THE ENCRPTION VALUE TO THE PORT ADAPTER" & "RECEIVE THE ENCRYPTION VALUE FOR THE HOST CONTROLLER"] to check if the second signal has been modified according to the common secret [Figure 389: "MATCH OF ENCRYPTION VALUES?"] (col 38, lines 6-14: *"In step 387, the host controller send the encryption value to the port adapter. In step 388, the port adapter receives the encryption value from the port adapter. In step 389, the port adapter compares the encryption value that it computed with the encryption value received from the host controller"*).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Lundkvist is directed to a method of controlling authorization to an object and a computer program product for the authorization control and Fig 33 of Blumenau et al is directed to "a "challenge-response" procedure used by the port adapter and host controllers of Fig. 32 to permit the port adapter to authenticate the identity of a host controller.

The fact that the Examiner may not have specifically responded to any particular arguments made by Applicant and Applicant's Representative, should not be construed as indicating Examiner's agreement therewith.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 5-11 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lundkvist (WO 02/035036 A1), hereinafter referred to as Lundkvist, in view of Blumenau et al (U.S. Pat 6493825 B1), hereinafter referred to as Blumenau.

Re claims 1 and 11: Lundkvist teaches a method for a first communication device [Fig 1, elt 1: vehicle] to performing authenticated distance measurement between said first communication device and a second communication device [Fig 1, elt 2: portable unit] (Abstract, lines 9-11), wherein the first and the second communication device share a common secret (Abstract: lines 9-13) and:

wherein the authenticated distance measurement comprises:

(means for) transmitting a first signal [Fig 3: first signal X] from the first communication device [Fig 1, elt 1: vehicle] to the second communication device [Fig 1, elt 2: portable unit] at a first time t1 (Fig 2, elt "MESSAGE X IS DETERMINED AND X IS

SENT" and elt: "←X→;" page 8, lines 11-17), said second communication device being adapted for receiving said first signal (Fig 2, elt "X IS RECEIVED AND DECRYPTED;" page 8, line 19), generating a second signal [Fig 2, elt "F(X) IS DETERMINED AND Y1 IS SENT" and elt: "←Y1—;" page 8, lines 20-21] by modifying the received first signal according to the common secret, and transmitting the second signal to the first communication device [Fig 2, elts: "X IS RECEIVED AND DECRYPTED," "F(X) IS DETERMIEND AND Y1 IS SENT" and "←Y1—" (page 8, lines 19-22);

(means for) receiving the second signal at a second time t2 (Fig 2, elt "Y1 IS RECEIVED, DECRYPTED, F(X) AND T1 ARE CHECKED"; page 8, lines 23-24); and (means for) determining the distance between the first and the second communication device according to a time difference between t1 and t2 (Fig 2, elt T1; page 3, lines 22-25; page 8, lines 24-28).

However, Blumenau teaches: (means for) generating by the first communication device [Fig 33, elt "STORAGE SUBSYSTEM PORT ADAPTER"] a third signal [Fig 33, elt 385] by modifying the first signal [Fig 33, elt 383] according to the common secret (col 37, lines 55-58); (means for) comparing the third signal [Fig 33, elt 385] with the received second signal [Fig 33, elts 387 & 388] to check if the second signal has been modified according to the common secret [Fig 33, elt 389] (col 37, line 59 – col 38, line 14).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Lundvist with the teachings of

Blumenau, for the purpose of providing expedient authentication as the authentication processes taught by Blumenau does not require decryption (see col 37, lines 60-62).

Re claim 5: The combination of Lundvist and Blumenau teaches the first signal [Lundvist: Fig 2, elt X] and the common secret are bit words and where the second signal [Lundvist: Fig 2, elt Y1] comprises information being generated by performing an XOR between the bit words (Lundvist: page 8, lines 1-2). The Examiner holds the Lundvist teaches symmetric key cryptography between the two exchanging parties. As such, Lundvist clearly anticipates the XOR cipher.

Re claim 6: The combination of Lundvist and Blumenau teaches the common secret has been shared before performing the distance measurement, the sharing comprises, performing an authentication check from the first communication device on the second communication device, by checking whether said second communication device is compliant with a set of predefined compliance rules (Lundvist: page 8, lines 19-28; in particular, lines 27-28 where the lock is unlocked if $E_SVAR = f(O_RND)$ where E_SVAR is a specific function of the first parties information and O_RND is a nonce generated by the verifier; see also the second embodiment: page 9, lines 1-13), if the second communication device is compliant, sharing said common secret by transmitting said secret to the second communication device (Lundvist: page 8, lines 27-28) (Blumenau: Fig 33; col 37, line 61 – col 38, line 14).

Re claim 7: The combination of Lundvist and Blumenau teaches the authentication check further comprises checking if the identification of the second device [E_ID] is compliant with an expected identification (page 9, lines 1-13;

particularly "control unit 70 creates namely a message that consists of identity information E_ID that is unique to the unit 2 and a random number E_RND ").

Re claim 8: Lundvist teaches a method of determining whether data stored on a first communication device [Fig 1, elt 1: vehicle] are to be accessed by a second communication device [Fig 1, elt 2: portable unit] (Abstract, lines 9-11), the method comprises performing an authenticated distance measurement between third communication device [Fig 1, elt 7] and the second communication device [Fig 1, elt 2: portable unit] (Abstract, lines 9-11; page 7, lines 7-9), wherein the third and the second communication device share a common secret (Abstract: lines 9-13), and

wherein the authenticated distance measurement comprises: transmitting a first signal [Fig 3: first signal X] from the third communication device [Fig 1, elt 7] to the second communication device [Fig 1, elt 2: portable unit] at a first time t1 (Fig 2, elt "MESSAGE X IS DETERMINED AND X IS SENT" and elt: " $\leftarrow X \rightarrow$;" page 8, lines 11-17), said second communication device being adapted for receiving said first signal (Fig 2, elt "X IS RECEIVED AND DECRYPTED;" page 8, line 19), generating a second signal [Fig 2, elt "F(X) IS DETERMINED AND Y1 IS SENT" and elt: " $\leftarrow Y1 \rightarrow$;" page 8, lines 20-21] by modifying the received first signal according to the common secret, and transmitting the second signal to the third device [Fig 1, elt 7; Fig 2, elts: "X IS RECEIVED AND DECRYPTED," "F(X) IS DETERMIEND AND Y1 IS SENT" and " $\leftarrow Y1 \rightarrow$ "] (page 8, lines 19-22);

receiving the second signal at a second time t2 (Fig 2, elt "Y1 IS RECEIVED, DECRYPTED, F(X) AND T1 ARE CHECKED"; page 8, lines 23-24); determining the

distance between the third and the second communication device according to a time difference between t1 and t2 (Abstract: lines 9-13; page 3, lines 17-20; page 4, lines 12-13); and checking whether said measured distance is within a predefined distance interval (page 3, lines 29-30).

However, Blumenau teaches: generating by the third communication device [Fig 33, elt "STORAGE SUBSYSTEM PORT ADAPTER"] a third signal [Fig 33, elt 385] by modifying the first signal [Fig 33, elt 383] according to the common secret (col 37, lines 55-58); comparing the third signal [Fig 33, elt 385] with the received second signal [Fig 33, elts 387 & 388] to check if the second signal has been modified according to the common secret [Fig 33, elt 389] (col 37, line 59 – col 38, line 14).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Lundvist with the teachings of Blumenau, for the purpose of providing expedient authentication as the authentication processes taught by Blumenau does not require decryption (see col 37, lines 60-62).

Re claim 9: The combination of Lundvist and Blumenau teaches the data stored on the first device are sent to the second device (Lundvist: Fig 2, elt "MESSAGE X IS DETERMINED AND X IS SENT") if it is determined that the data stored on the first device are to be accessed by the second device (Lundvist: Fig 2, elt "TRIPPING DEVICE IS ACTUATED;" page 5, lines 17-19).

Re claim 10: The combination of Lundvist and Blumenau teaches the first communication device [Lundvist: Fig 1, elt 1] comprises the third communication device [Lundvist: Fig 1, elt 7] (page 7, lines 7-10).

Re claim 13: The combination of Lundkvist and Blumenau teaches means for playing back multimedia content based on a result of the authenticated distance measurement (Blumenau: col 5, lines 22-25 & lines 37-38; col 7, lines 47-50).

5. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lundkvist (WO 02/035036 A1), hereinafter referred to as Lundkvist, in view of Blumenau et al (U.S. Pat 6493825 B1), hereinafter referred to as Blumenau, in further view of Rofheart et al (WO 01/93434 A2), hereinafter referred to as Rofheart.

Re claim 3: The combination of Lundkvist and Blumenau teaches all the limitations of claim 1 as previously discussed. However, Rofheart teaches the first signal is a spread spectrum signal (page 15, line 31 – page 16, line 4).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Lundkvist and Blumenau to utilize spread spectrum signals, as taught by Rofheart, for the purpose of providing increased resistance to natural & artificial interference and to prevent signal detection (page 16, lines 8-13).

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully

consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Pat 4438824 A [Figure 3]

U.S. Pat Pub 2001/0043702 A1 [Figure 4]

U.S. Pat Pub 2003/0220765 A1

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 8am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435